June 9, 2011 NIST Smart Grid Privacy Subgroup Meeting Notes

Minutes by Rebecca Herold

Please send this distribution list any necessary corrections or additions.

Next full group teleconference meeting:

Thursday June 23, 2011 at 11:00am est

Here are my summary notes from the meeting:

1. Past meeting notes
- See http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGPrivacy
- Note the spiffy new look!

2. Team Updates

- Each team leader will provide the following information:
  - Overview of the team's work
  - Current status of any content/paper/etc. the team is working on, including anticipated completion date/timeframe
  - How your newly created content/paper/etc. will be used. E.g., target groups, distribution paths, etc.

- NSTIC Team: Krystina Schaefer, (team lead)
  - Krystina (Via Email):
    - At the June 2nd meeting we talked about some of the difficulties in creating an effective deliverable from the NSTIC document because it is so high-level. The team was originally created at the request of DOE to identify privacy risks of applying the NSTIC authentication and identification methods to the Smart Grid, in a white paper format. We also touched on some of the various issues surrounding implementation of the Strategy itself.
    - At this point the main issue is finding clarity over what the appropriate next steps are. Since the governance meeting is June 9th and 10th, the group is going to regroup on June 16th (11:00 am EST) to hear thoughts from those who were able to attend the meeting and determine the best way to proceed, based on the feedback received. So, if you are attending the meeting or have any thoughts on the matter feel free to join the call!
    - NSTIC Call
      - June 2nd @ 11:00 am EST
      - Call #: 866-802-3515
      - Participant code: 2817109#

- Third Party Team: Brent Struthers (team lead) will include discussion of relationship to the NAESB document

- o Tanya: Have a copy of a non-NAESB version of the NAESB document to add details for what is missing in that document with regard to recommendations. Call tomorrow at 2pm est to discuss.
  - o Ken: Is the team filing comments to the NAESB document?
  - o Tanya: I personally will not be. No discussion about the team yet.
  - o Rebecca: Can the team submit one set on behalf of our NIST team?
  - o Tanya: Cannot see why not.
  - o Rebecca and Tanya met with Jonathan Booe to ensure they knew what our NIST group was doing, and make sure they were fine with that.
  - o Tanya: Provided overview and said we wanted to provide more details, but wanted to make sure that NAESB was okay with that. He said that was fine.

- Privacy Use Cases Team: Christine Hertzog, Smart Grid Library (team lead)
  - o Christine H: Been slowly going forward. Had team meeting earlier. Time consuming to discuss each use case and getting each reviewed.
  - o Have a plan to expedite and shrink team to those who can commit to do the work and get the use cases done. Moving to a weekly meeting instead of bi-weekly.

- PEV Team: Mike Coop, Hey Coop! (team lead)
  - o Tanya: Chris K has done work on Stan Klein's outline created for the PEV roaming team to point out where the privacy issues may exist.
  - o Has a 2-page document. If anyone wants in, let us know. Done with calls until sometime in August.

- Training and Awareness Team: Rebecca Herold (team lead)
  - o Rebecca: Described what team did earlier this week, and plans are going forward.
  - o Ken Wacks: Gut reaction from marketing, they want to make money at the same time that they want to do awareness raising of privacy issues.
  - o Rebecca: Parallels with info security
  - o Franco: Also looking at providing service, privacy impacts that are involved should be identified.

- Miscellaneous
  - o Meetings are the 2nd and 4th Thursdays of each month. Next full group meeting will be Thursday, June 23.
  - o Other?
    - ▪ Rebecca: Described being asked for sensitive personal information from a large financial company that had contacted her and asked her to do an interview, for no pay. How are utilities and other smart grid entities doing background checks? On non-employees and non-customers?
      - • Franco: Due diligence; give them fake ID to just let them check their boxes.
      - • Ken Wacks: Don't game the system, tell them to change the process.
      - • Michelle Drgn: Asked for SSNs because they could; traveling; asked for SSN from Fortune 500 that had privacy practices in place. Could be a trend where organizations are trying to legally cover themselves.
      - • Martha: In future conversations, when president gives me their info, then I'll give him mine
      - • Sarah: Large organizations have a problem to solve. Not looking at background adequately. Need to know why they have a liability problem.

- Rebecca: But organizations feel it is okay to invade privacy as long as it is not against the law. Many of the same issues we revealed for the smart grid privacy issues.
- Ken Wacks: A substitute is looking online.
- Sarah: Disagree, liability issues go beyond just looking online.
- Ken Wacks: Who cares?
- Sarah: Looking online may not reveal criminal activity for legitimate professionals
- Michelle: Don't most interviews have a disclaimer at the end of the article?
- Sarah: Normal press issues.
  - Marty: Started talking about NAESB third party data sharing document. REQ-21. Anyone aware of that standard?
    - Tanya: About interface? Yes, Rebecca has been forwarding that info
    - Marty: Place holder in appendix for security and privacy. That section is empty. Currently it has use cases, usage model based upon PAP10, etc. Orchestrating exchange by 3rd parties. Task force has elected to build messaging on top of Internet standards. Would be helpful to committee and downstream if our group could provide input to these changes from the CSWG perspective and the suitability of these Internet standards to meet those controls. Interest in looking at?
    - Rebecca: Other CSWG groups looking at?
    - Marty: Know we are doing a lot. This could be a showcase. It is looking at all the issues dealing with information security and privacy. Not very deep. Likelihood of being adopted quickly by all municipalities. Promoting concept that this would be valuable to get our input on and this is a pivotal time. Comment period ends Monday. Number of weeks between when it goes out for a formal review.
    - Sandy: Go ahead and send formal request from PAP10 to Marianne, Frances and myself to put into the queue for the subgroups. May get to by end of July.
    - Marty: That won't be enough time.
    - Tanya: They need help putting privacy protections in, or assessing what would be sufficient privacy protections. Not pointing to the REQ-22?
    - Marty: Yes.
    - Tanya: trying to determine how we can help in a shortframe
    - Marty: What would be great is a list of RFCs. A set of controls associated with each RFC, and with the privacy standard from RFC 22, could show there is a correlation between those controls and there is adequate coverage. A table mapping them and showing adequate controls.
    - Tanya: Focus just on privacy?
    - Marty: Not sure. Not sure if it is he privacy group alone, or there should be more.
    - Sandy: Could be a privacy perspective, but should go through the standards subgroup.
    - Tanya: Maybe could assist by looking at just the privacy issues.
    - Marty: REQ 22 can be represented by the set of NISTIR 7628 controls?
    - Tanya: Hard to say
    - Marty: How to analyze for sufficiency?

- Sandy: Read the standard, look at scope and context, then literally map to all 175 or so NISTIR requirements. Is it adequately covered, or not even in the NISTIR, or is totally a mismatch?
- Tanya: Trying to map 22, 3rd party, to NISTIR would be difficult. Part of basis is not the high level requirements. REQ 22 only deals with privacy. Doesn't go into security. So, could we map REQ 22 in same way, would be hard. If REQ 21, our group may be able to help the standards group. Look sufficient? Etc. However, the security review would need to go through standards group.
- Michelle D: Part of a group that could provide some input. Will email info (hard to hear).
- Rebecca: SO how should we do this?
- Tanya: After standards group gets it, then we need to see how we can be involved. Will be job of standards to do that actual security review, and then we can assist when they are doing this. Will be sometime this summer. Not sure when. Think about if group members have time in the coming weeks we may be able to tweak template to address the privacy issues. Group think about if they can give 10 – 20 hours to provide input on this. Certainly anyone who wants to look at document, please look at it and see if you want to participate. Some is highly technical, but others can be addressed and can provide comments.
- Rebecca: Sent info to group. Recap.
- Marty: Will send email as Sandy asks.
- Tanya: Get into queue as early as possible. There are many things/requests coming in.
- Rebecca: Events; send info to me
- Tanya: Anyone going to Montreal SGIP meeting?
  - OH PUC: NOT going to Montreal; going to another at that time.
  - Tanya: IF anyone wants details let me know. In mid-July in Montreal with SGIP sister.

Thanks,

Rebecca